

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-260630

(43)Date of publication of application : 29.09.1998

(51)Int.Cl. G09C 1/00  
G09C 1/00  
H04L 9/08

(21)Application number : 10-007018

(71)Applicant : N T T DATA TSUSHIN KK  
NIPPON TELEGR & TELEPH CORP  
<NTT>

(22)Date of filing : 16.01.1998

(72)Inventor : TAKAHASHI YOSHIO  
MORIHATA HIDEMI

(30)Priority

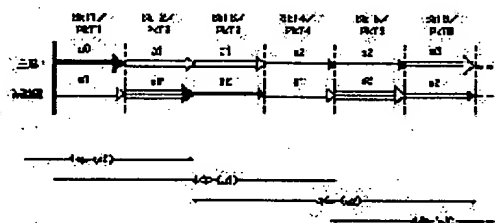
Priority number : 09 6810 Priority date : 17.01.1997 Priority country : JP

## (54) METHOD AND SYSTEM FOR KEY MANAGEMENT FOR ELECTRONIC SIGNATURE

(57)Abstract:

PROBLEM TO BE SOLVED: To eliminate the need to stop issuing an electronic signature at the time of update or limit the use of services after update by preparing keys used for a signature key, updating those keys according to a certain rule, and updating and making open a confirmation key in synchronism with the update of those keys.

SOLUTION: Two keys are both given an update object period of one year, a safe use period of five years, and four-year update cycles, and used as auxiliary key in the starting year and ending year and a main key in intermediate two years. Key update is performed at the start point of the final one year wherein one key is continuously the main key. At the end point of the use section of one key, the use suction of an update key is started. When the key update is performed for a key SkT for signature, a corresponding key PkT for confirmation is also updated synchronously. To issue a membership registration note, the main key for signature is used and to confirm the membership registration note, one of a pair of the main key for confirmation and an auxiliary key for confirmation is used.



## LEGAL STATUS

[Date of request for examination] 18.01.2001

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than

the examiner's decision of rejection or  
application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision  
of rejection]

[Date of requesting appeal against examiner's  
decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-260630

(43) 公開日 平成10年(1998) 9月29日

(51) Int.Cl. <sup>6</sup>	識別記号	F I	
G 0 9 C 1/00	6 3 0	G 0 9 C 1/00	6 3 0 Z
	6 4 0		6 3 0 F
			6 4 0 B
			6 4 0 D
H 0 4 L 9/08		H 0 4 L 9/00	6 0 1 Z
審査請求 未請求 請求項の数24 O L (全 16 頁) 最終頁に続く			

(21) 出願番号 特願平10-7018

(22) 出願日 平成10年(1998) 1月16日

(31) 優先権主張番号 特願平9-6810

(32) 優先日 平9 (1997) 1月17日

(33) 優先権主張国 日本 (J P)

(71) 出願人 000102728

エヌ・ティ・ティ・データ通信株式会社  
東京都江東区豊洲三丁目3番3号

(71) 出願人 000004226

日本電信電話株式会社  
東京都新宿区西新宿三丁目19番2号

(72) 発明者 高橋 芳夫

東京都江東区豊洲三丁目3番3号 エヌ・  
ティ・ティ・データ通信株式会社内

(72) 発明者 森島 秀実

東京都新宿区西新宿3丁目19番2号 日本  
電信電話株式会社内

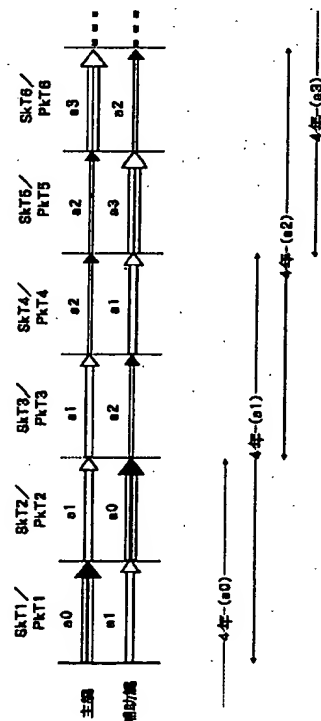
(74) 代理人 弁理士 鈴木 正剛

(54) 【発明の名称】 電子署名用の鍵管理方法及びシステム

(57) 【要約】

【課題】 署名鍵を更新する際に電子署名の発行を停止したり、サービス提供を制限する必要がない、電子署名用の鍵管理方法を提供する。

【解決手段】 異なる時期に同一の更新周期で更新される2個の鍵を電子署名用の署名鍵（主鍵・補助鍵）として用意しておき、各鍵の更新周期を例えば3つの区間に分割し、更新後の最初及び最後の区間を補助鍵としての区間、中間の区間を主鍵としての区間とし、主鍵で電子署名を行う。この電子署名の確認は、署名鍵として使用されるこの2個の鍵の更新に同期して更新される2個の確認鍵のいずれかで行う。



## 【特許請求の範囲】

【請求項1】 各々異なる時期に周期的に内容が更新される複数の鍵を用意しておき、前記複数の鍵を、各々の鍵の更新周期よりも短い切替周期で1個ずつ切り替え、切り替えた鍵を電子署名用の署名鍵としての使用に供することを特徴とする、電子署名用の鍵管理方法。

【請求項2】 前記切替周期がすべての鍵について同一長さの期間であることを特徴とする、請求項1記載の鍵管理方法。

【請求項3】 各々異なる時期に周期的に内容が更新される複数の鍵について、個々の鍵の更新周期を3つの区間に分割して最初及び最後の分割区間を予備区間、中間の分割区間を電子署名用の署名鍵として使用するための使用区間とし、各鍵についての前記使用区間を、他の鍵の使用区間と時間的に連続させ且つ互いに重複しないように切り替えることを特徴とする、電子署名用の鍵管理方法。

【請求項4】 前記署名鍵に基づく電子署名の有効期間が、前記最初の分割区間と最後の分割区間のうち短い方の区間以下の長さの期間であることを特徴とする、請求項3記載の鍵管理方法。

【請求項5】 各鍵についての前記最初及び最後の分割区間の和が当該鍵についての前記中間の分割区間と同じ長さの期間であることを特徴とする、請求項3記載の鍵管理方法。

【請求項6】 各鍵についての前記最初の分割区間と最後の分割区間とがそれぞれ同じ長さの期間であることを特徴とする、請求項3記載の鍵管理方法。

【請求項7】 一の鍵についての最後の分割区間と他の鍵についての最初の分割区間とが同じ長さの区間であることを特徴とする、請求項3記載の鍵管理方法。

【請求項8】 一の鍵についての前記使用区間中に他の鍵を更新しておき、前記一の鍵についての前記使用区間の終了時点で前記更新された他の鍵についての前記使用区間を開始させることを特徴とする、請求項3記載の鍵管理方法。

【請求項9】 前記複数の鍵の各々が、前記切り替えにかかわらず、前記署名鍵としての使用が可能なものであることを特徴とする、請求項1または3記載の鍵管理方法。

【請求項10】 周期的に更新される第1の鍵と、この第1の鍵と異なる時期に周期的に更新される第2の鍵とを用意しておき、前記第1の鍵及び第2の鍵のいずれかを、各々の鍵の更新周期よりも短い切替周期で交互に切り替えて、電子署名用の署名鍵としての使用に供するとともに、前記第1の鍵の更新時期に同期して更新され当該第1の鍵が署名鍵のときに確認鍵となる第3の鍵と、前記第2の鍵の更新時期に同期して更新され当該第2の鍵が署名鍵のときに確認鍵となる第4の鍵とをペアで公開し、

前記第3の鍵及び第4の鍵のペアを前記電子署名の確認用に供することを特徴とする、電子署名用の鍵管理方法。

【請求項11】 前記第3の鍵及び第4の鍵に各々当該鍵の使用終了期限を付加することを特徴とする、請求項10記載の鍵管理方法。

【請求項12】 前記更新周期が、当該鍵の安全性が確保できる平均的な期間から当該鍵をもとに生成した電子署名の有効期間を減じた期間以下であることを特徴とする、請求項1、3または10記載の鍵管理方法。

【請求項13】 それぞれ異なる時期に周期的に更新されるM個(Mは2以上の自然数)の署名鍵を用意するとともに、個々の署名鍵の更新時期に同期して更新されるM個の確認鍵を同時期に公開する段階と、前記用意したM個の署名鍵から1個の署名鍵を当該署名鍵の更新周期よりも短い周期で所定順に選択して所定の署名対象データの電子署名を行う段階と、前記公開されたM個の確認鍵のいずれかをを用いて前記電子署名を確認する段階とを含む、電子署名用の鍵管理方法。

【請求項14】 電子署名の署名鍵として用いる複数の鍵を保持する鍵保持手段と、前記複数の鍵の内容をそれぞれ異なる時期に周期的に更新する鍵更新手段と、前記鍵更新手段でその内容が更新された鍵を所定規則に従って前記鍵保持手段より読み出し、読み出した鍵を前記署名鍵として、所定の署名対象データについての電子署名を行う署名手段と、を備えたことを特徴とする、電子署名用の鍵管理システム。

【請求項15】 電子署名の署名鍵として用いる第1の鍵及び第2の鍵を保持する鍵保持手段と、前記第1の鍵及び第2の鍵の内容をそれぞれ異なる時期に同一周期で更新する鍵更新手段と、前記鍵更新手段でその内容が更新された鍵を所定規則に従って前記鍵保持手段より読み出し、読み出した第1または第2の鍵を前記署名鍵として、所定の署名対象データについての電子署名を行う署名手段と、を備えたことを特徴とする、電子署名用の鍵管理システム。

【請求項16】 前記第1の鍵に同期して更新され当該第1の鍵が署名鍵であるときの確認鍵となる第3の鍵、及び前記第2の鍵に同期して更新され当該第2の鍵が署名鍵であるときの確認鍵となる第4の鍵を保持する鍵保持手段を備え、前記第1の鍵または第2の鍵を用いて前記電子署名を行ったときに前記第3の鍵及び第4の鍵を同時期に公開するように構成されていることを特徴とする、請求項15記載の鍵管理システム。

【請求項17】 前記鍵更新手段は、前記更新期間を3区間に分割するとともに、各鍵の更新を当該鍵について

の分割区間よりも短い時間内に行うように構成されていることを特徴とする、請求項14または15記載の鍵管理システム。

【請求項18】 前記鍵更新手段は、一つの分割区間の鍵内容を後続の分割区間に引き継ぐ第1のモードと、直前の分割区間から後続の分割区間に移行する際に直前の分割区間の鍵内容を互いに置換する第2のモードとを選択して適用するモード選択手段とを有し、一つの鍵について前記第1のモードを適用しているときに他の鍵の鍵内容を更新するように構成されていることを特徴とする、請求項17記載の鍵管理システム。

【請求項19】 前記署名手段は、前記複数の鍵の各々について、更新後の最初の分割区間の終期から最後の分割区間の始期までの間、当該鍵を電子署名用の署名鍵として用いるように構成されていることを特徴とする、請求項17記載の鍵管理システム。

【請求項20】 前記電子署名が会員間で会員認証に用いられる場合、前記署名手段は、前記署名対象データに、当該電子署名の有効期間と当該会員の署名確認鍵を含む個人情報とを含めて前記電子署名を行うように構成されていることを特徴とする、請求項14または15記載の鍵管理システム。

【請求項21】 前記電子署名が会員間で使用可能な電子チケットの認証に用いられる場合、前記署名手段は、前記署名対象データに、当該電子チケットに基づくサービスを識別するための情報と会員の署名確認鍵とを含めて前記電子署名を行うように構成されていることを特徴とする、請求項14または15記載の鍵管理システム。

【請求項22】 前記署名対象データに、当該電子チケットに基づくサービス情報の提供主体が管理する通番情報をさらに含めることを特徴とする、請求項21記載の鍵管理システム。

【請求項23】 M個(Mは2以上の自然数)の署名鍵のいずれかによって生成された電子署名と、前記電子署名に用いられた署名鍵を含むM個の署名鍵の更新に同期して更新されるM個の確認鍵を受領する署名受領手段と、前記受領した電子署名を前記M個の確認鍵のいずれかで確認する署名確認手段とを備え、前記署名確認手段で確認がとれた電子署名を正当と判定することを特徴とする、電子署名の認証システム。

【請求項24】 M個(Mは2以上の自然数)の署名鍵のうち異なる時期に更新された署名鍵によって生成された複数の電子署名と、前記複数の電子署名に用いられた署名鍵を含むM個の署名鍵の更新に同期して更新されるM個の確認鍵を受領する署名受領手段と、前記受領した電子署名を前記M個の確認鍵のいずれかで確認する署名確認手段とを備え、前記署名確認手段で確認がとれた電子署名を正当と判定することを特徴とする、電子署名の認証システム。

#### 【発明の詳細な説明】

##### 【0001】

【発明の属する技術分野】本発明は、電子署名の発行や電子署名に基づく種々のサービスの提供等を制限することなく、電子署名用の鍵の内容を更新することを可能とする、電子署名用の鍵管理方法、及びこの鍵管理方法の実施に適したシステムに関する。ここに、電子署名とは、利用者固有の鍵を用いて利用者本人であることを証明する電子的な署名をいう。

##### 【0002】

【従来の技術】例えば会員証によって会員が特定される会(あるいは団体)において、会員相互で会員証の正当性を評価できるようにすることは、会の運営上、極めて重要なことである。最近では、会員証を例えばICカードのような高セキュリティ性の媒体の形で発行して会員のみが所持し得る電子身分証明書としたり、オンライン上で、電子署名技術を用いて偽造の困難な会員登録証(電子身分証明書)や電子チケットとすることが試みられている。

【0003】会員登録証や電子チケット等(以下の説明では、便宜上、会員登録証と称する)は、内容の真性評価はもとより、会員登録証を使用する者が会員本人であることを正しく確認できるようにしておくことが必要である。そのため、従来は、本人しか生成できない電子署名を用いてその会員登録証が偽造されていないかどうか、あるいは、その会員登録証の所持者が正当な会員かどうかを確認することが行われている。

【0004】電子署名には、通常、公開鍵方式による暗号化技術が利用される。すなわち、所定の会員登録機関が自機関の秘密鍵(署名鍵)を用いて電子署名を行い、その署名鍵に対応する公開鍵(確認鍵)をすべての会員に対して配布する。各会員が電子署名の認証を行う場合は、確認鍵を用いて電子署名を確認する。なお、確認鍵自体には、会員登録機関の正当な公開鍵であることを表す情報が含まれていないので、予め確認鍵の正当性を別途確認しておく必要がある。

【0005】上述の公開鍵方式では、安全性の根拠の一つを、解読の際の計算量の多さにおいている。従って、同一の署名鍵や確認鍵を長期間使用し続けることは安全性の低下につながるため、各鍵は、一定期間ごとに更新することが望ましい。そのため、従来は、署名鍵を定期的に更新できるようにし、その際に、署名鍵の更新に同期して更新された確認鍵を各会員が入手できるようにしているのが一般的である。

【0006】更新された確認鍵を入手する手段としては、会員登録機関が、会員全員に新しい確認鍵を同時に配布することが考えられる。また、新しい確認鍵を所定の公開鍵証明書発行センタに登録することも考えられる。後者の場合、公開鍵証明書発行センタで、署名対象データを自己の秘密鍵(センタ秘密鍵)で署名して公開

鍵証明書とし、適宜、この公開鍵証明書を会員に配布する。配布された会員は、予め通知された公開鍵証明書発行センタの公開鍵（センタ公開鍵）で電子署名を確認する。

【0007】ある会員が、自分の会員登録証を第三者に確認してもらいたい場合は、会員が公開鍵証明書を取得し、取得した公開鍵証明書をその会員登録証に添付する。これにより、電子署名を確認する側では、新たな会員登録機関の公開鍵の正当性を容易に確認できるようになる。なお、公開鍵証明書は、電子署名に常に添付しなければならないというのではなく、署名鍵及び確認鍵が更新されたときに1回だけ添付すれば足りるものである。

【0008】ある会員が他の会員に対してオンラインで会員登録証を送信する場合は、送信時のデータ量を少なくするために、公開鍵証明書の添付を省略する場合がある。この場合、公開鍵証明書は、受信した会員の側で取得することになる。いずれにしても、公開鍵証明書を用いようとする場合は、確認鍵が更新される度に、会員登録証を利用する会員、あるいはその会員登録証を確認する会員が公開鍵証明書発行センタにアクセスして公開鍵証明書を取得する必要がある。

【0009】

【発明が解決しようとする課題】上述のように、署名鍵が更新された場合は、以下のいずれかの行為が、会員登録機関と会員との間、あるいは会員相互間で行われる。

(1) 会員登録機関が全会員に新しい確認鍵を配布する。

(2) ある会員が最初に会員登録証を利用する際に、公開鍵証明書を取得して添付する。

(3) 電子署名を確認する会員側で、適宜公開鍵証明書を取得する。

【0010】しかしながら、上記の三つの形態では、それぞれ下記の問題が発生する。

(1) の形態では、会員登録機関で鍵更新処理を行う場合、全利用者が一斉に新しい確認鍵を取得しようとして会員登録機関にアクセスするため、会員登録機関側に備えられるシステムにそのための処理が集中してしまい、システムの動作が不安定になるおそれがある。特に、会員数が非常に多い場合は、鍵更新後は、全利用者に新しい鍵を配布し終わるまでは会員登録証の発行を停止させなければならない。

(2) の形態では、送受信の際のデータ量が増大するとともに、公開鍵証明書の取得のための時間が余分にかかる。また、公開鍵証明書が偽造されると、偽りのセンタ公開鍵が配布されてしまうので、リスクが公開鍵証明書発行センタにおけるセンタ公開鍵の安全性に依存することになる。

(3) の形態では、電子署名を確認する会員、例えばある会員の会員登録証を確認して何らかのサービスを提供

しようとする会員は、ある会員の会員登録証を受信してから、公開鍵証明書を取得することになる。そのため、鍵更新後、ある会員が初めて会員登録証の確認を求める場合、公開鍵証明書を取得して会員登録証を確認するまで、当該他の会員は、サービス提供を制限するしかない。また、公開鍵証明書の取得を即時に行うために、公開鍵証明書発行センタまたは会員登録機関にオンライン・アクセスする場合には、その分、通信費が増加することになる。

【0011】このように、従来は、署名鍵が更新される度に、いずれかのシステムの運用に悪影響を与えたり、会員のサービス利用が制限される等の不具合があった。

【0012】本発明の課題は、上記不具合のない、電子署名用の鍵管理方法を提供することにある。本発明の他の課題は、上記鍵管理方法の実施に適したシステムを提供することにある。

【0013】

【課題を解決するための手段】本発明の鍵管理方法は、各々異なる時期に周期的に内容が更新される複数の鍵を用意しておき、前記複数の鍵を、各々の鍵の更新周期よりも短い切替周期で1個づつ切り替え、切り替えた鍵を電子署名用の署名鍵としての使用に供することを特徴とする。前記切替周期は、例えば、すべての鍵について同一長さの期間とすることが、鍵更新を容易ならしめる上で効果的である。

【0014】本発明の他の鍵管理方法は、各々異なる時期に周期的に内容が更新される複数の鍵について、個々の鍵の更新周期を3つの区間に分割して最初及び最後の分割区間を予備区間、中間の分割区間を電子署名用の署名鍵として使用するための使用区間とし、各鍵についての前記使用区間を、他の鍵の使用区間と時間的に連続させ且つ互いに重複しないように切り替えることを特徴とする。

【0015】本発明の他の鍵管理方法は、周期的に更新される第1の鍵と、この第1の鍵と異なる時期に周期的に更新される第2の鍵とを用意しておき、前記第1の鍵及び第2の鍵のいずれかを、各々の鍵の更新周期よりも短い切替周期で交互に切り替えて、電子署名用の署名鍵としての使用に供するとともに、前記第1の鍵の更新時期に同期して更新され当該第1の鍵が署名鍵のときに確認鍵となる第3の鍵と、前記第2の鍵の更新時期に同期して更新され当該第2の鍵が署名鍵のときに確認鍵となる第4の鍵とをペアで公開し、前記第3の鍵及び第4の鍵のペアを、前記電子署名の確認用に供することを特徴とする。この場合、前記第3の鍵及び第4の鍵に各々当該鍵の使用終了期限を付加するようにしても良い。

【0016】なお、前記更新周期は、当該鍵の安全性が確保できる平均的な期間から当該鍵をもとに生成した電子署名の有効期間を減じた期間以下とする。

【0017】本発明の他の鍵管理方法は、それぞれ異な

る時期に周期的に更新されるM個（Mは2以上の自然数）の署名鍵を用意するとともに、個々の署名鍵の更新時期に同期して更新されるM個の確認鍵を同時期に公開する段階と、前記用意したM個の署名鍵から1個の署名鍵を当該署名鍵の更新周期よりも短い周期で所定順に選択して所定の署名対象データの電子署名を行う段階と、前記公開されたM個の確認鍵のいずれかをを用いて前記電子署名を確認する段階とを含む。

【0018】上記各鍵管理方法は、電子署名の署名鍵として用いる複数の鍵を保持する鍵保持手段と、前記複数の鍵の内容をそれぞれ異なる時期に周期的に更新する鍵更新手段と、前記鍵更新手段でその内容が更新された鍵を所定規則に従って前記鍵保持手段より読み出し、読み出した鍵を前記署名鍵として、所定の署名対象データについての電子署名を行う署名手段と、を備えた電子署名用の鍵管理システムによって実施可能である。

【0019】また、電子署名の署名鍵として用いる第1の鍵及び第2の鍵を保持する鍵保持手段と、前記第1の鍵及び第2の鍵の内容をそれぞれ異なる時期に同一周期で更新する鍵更新手段と、前記鍵更新手段でその内容が更新された鍵を所定規則に従って前記鍵保持手段より読み出し、読み出した第1または第2の鍵を前記署名鍵として、所定の署名対象データについての電子署名を行う署名手段と、を備えた鍵管理システムも、本発明の鍵管理方法を実施するうえで好適となる。このような鍵管理システムにおいて、好ましくは、前記第1の鍵に同期して更新され当該第1の鍵が署名鍵であるときの確認鍵となる第3の鍵、及び前記第2の鍵に同期して更新され当該第2の鍵が署名鍵であるときの確認鍵となる第4の鍵を保持する鍵保持手段をさらに備え、前記第1の鍵または第2の鍵を用いて前記電子署名を行ったときに前記第3の鍵及び第4の鍵を同時期に公開するように構成する。

【0020】本発明は、また、電子署名鍵と確認鍵とを受領したときに、当該電子署名が正当なものかどうかを判定することができる、電子署名の認証システムを提供する。この認証システムは、M個（Mは2以上の自然数）の署名鍵のいずれかによって生成された電子署名と、前記電子署名に用いられた署名鍵を含むM個の署名鍵の更新に同期して更新されるM個の確認鍵を受領する署名受領手段と、前記受領した電子署名を前記M個の確認鍵のいずれかで確認する署名確認手段とを備え、前記署名確認手段で確認がとれた電子署名を正当と判定することを特徴とする。署名受領手段は、M個の署名鍵のうち異なる時期に更新された署名鍵によって生成された複数の電子署名と、前記複数の電子署名に用いられた署名鍵を含むM個の署名鍵の更新に同期して更新されるM個の確認鍵を受領するように構成しても良い。この認証システムで確認がとれた場合は、当該電子署名が少なくとも本発明の鍵管理システムで生成されたことが容易にわ

かる。

#### 【0021】

【発明の実施の形態】以下、本発明の実施の形態を図面を参照して説明する。まず、本発明が適用される会員システムの概略を説明する。この会員システムは、例えば、会員のみが操作可能な複数の会員操作システムと、会員を統括管理する会員登録機関に備えられる会員登録システムと、公開鍵証明書発行センタとをそれぞれ双方向通信可能な形態、例えば図示しない通信手段を公衆網を通じて接続し、認証通信（authenticated communication）によって鍵配布を行うものである。但し、各会員操作システムと会員登録システムとの間で認証通信が可能である場合、公開鍵証明書発行センタは、必ずしも必要ではない。

【0022】認証通信には、共通鍵方式、つまり署名鍵と確認鍵とが同一鍵である方式も採用可能であるが、以下の説明では、便宜上、前述の公開鍵方式を用いることを前提とする。

【0023】会員登録システムは、会員からの会員登録請求情報に応じて会員登録を行う機能と、登録した各会員に対して自機関の秘密鍵（つまり署名鍵）を用いて会員登録証を発行する機能と、署名鍵を定期的に更新する機能と、署名鍵に対応する公開鍵（つまり確認鍵）を生成及び更新する機能とを有する。これらの機能の詳細については、後述する。

【0024】公開鍵証明書発行センタは、会員登録機関名、会員登録システムが生成した確認鍵、その他の情報（署名アルゴリズムや署名の有効期間等）を署名対象データとして、自己の秘密鍵（センタ秘密鍵）で電子署名を生成し、これを公開鍵証明書として保持するとともに、この公開鍵証明書を会員からの求めに応じて適宜発行するものである。

【0025】各会員操作システムは、会員登録システムから直接あるいは公開鍵証明書発行センタを通じて確認鍵を取得し、会員登録申請を行うものである。なお、公開鍵証明書発行センタを通じて取得する場合は、公開鍵証明書を公開鍵証明書発行センタの公開鍵（センタ秘密鍵）で確認するための処理が必要となる。

【0026】なお、以下の説明では、システム構成やその構成要素を示す必要がある場合を除き、会員操作システムを「会員」、会員登録システムを「会員登録機関」、公開鍵証明書発行センタを「センタ」と称する。

【0027】図1は、会員登録機関、会員、センタ間で行われる鍵、その他の電子情報の授受の様子を模式的に表した図である。センタCAに関する部分は、既に述べたように不可欠ではないが本例では使用する、という意味で、破線で示してある。図1において、「SkT1」、「SkT2」は更新前後の署名鍵、「PkT1」、「PkT2」は確認鍵、「SkCA」はセンタ秘密鍵、「PkCA」はセンタ公開鍵、「CERT」は公

開鍵証明書、「L1, L2」は会員U1, U2に対して発行される会員登録証である。署名鍵(SkT1, SkT2)による電子署名は、会員登録証の発行の際に行われる。以後の説明で、会員登録証の発行という場合は、電子署名と同義とする。

【0028】図1における鍵等の配送シーケンスは図2に示すとおりである。前提として、会員U1, U2は、センタ公開鍵PkCAを予め取得し、公開鍵証明書を取得したときに公開鍵証明書を確認できるものとする。

【0029】まず、会員登録機関Tで署名鍵SkT1、及び確認鍵PkT1を用意する(ステップS101)。確認鍵PkT1については、センタCAに登録しておく(ステップS102, S103)。会員U1は、センタCAから公開鍵証明書CERT(PkT1)を取得した後(ステップS104)、会員登録機関Tに会員登録申請を行う。その際、自己の確認鍵(PkU1)を送出する(ステップS105)。会員登録機関Tは、この会員の確認鍵(PkU1)とその他の情報に対し、署名鍵SkT1を用いて会員登録証L1を発行する(ステップS106)。

【0030】所定期間経過後、会員登録機関Tでは、署名鍵SkT1を署名鍵SkT2に更新する(ステップS107)。そして、更新後の署名鍵SkT2に対応する確認鍵PkT2を、センタCAに再登録する(ステップS108, S109)。会員U2は、センタCAから公開鍵証明書CERT(PkT2)を取得した後(ステップS110)、会員登録機関Tに会員登録申請を行う。その際、自己の確認鍵(PkU2)を送出する(ステップS111)。会員登録機関Tは、この会員登録申請に対し、署名鍵SkT2を用いて会員登録証L2を発行する(ステップS112)。その後、会員U1, U2が、会員登録証L1, L2に基づく相互認証を行う(ステップS113)。

【0031】このようにして鍵等が配送される場合において、少なくとも下記のことを行えるようにする。

(1) 会員登録機関Tが、会員登録証の発行を中断せずに、署名鍵SkTや確認鍵PkTを定期的に更新したい。

(2) 会員U1, U2間で、署名鍵SkT1を用いて発行された会員登録証L1と、署名鍵SkT2を用いて発行された会員登録証L2とをオフラインで正しく相互確認したい。

(3) 会員登録証L1, L2の確認の際に付加情報、例えば公開鍵証明書CERT(PkT)等を相手側に送る手間を無くしたい。

【0032】これらを解決するために会員登録機関Tにおいて行う本発明の鍵管理方法を、以下に説明する。まず、最も単純な例として、2個の鍵の一方を主鍵、他方を補助鍵として、両者を一定の規則に従って切り替えながら電子署名の署名鍵とし、電子署名の確認には、2個

の署名鍵に対応する2個の確認鍵をペアで用いる場合の例を挙げる。つまり、署名鍵SkT、確認鍵PkTを、それぞれ主鍵、補助鍵の2個ずつ用意する。以下、説明上、主鍵と補助鍵とを区別する必要がある場合は、主鍵としての署名鍵SkTを署名用主鍵、補助鍵としての署名鍵SkTを署名用補助鍵、主鍵としての確認鍵PkTを確認用主鍵、補助鍵としての確認鍵PkTを確認用補助鍵と称する。

【0033】各鍵は、それぞれ異なる時期に周期的に更新される。更新周期は、必ずしも同一期間である必要はない。また、各鍵には、それぞれ安全に使用できる平均的な期間(安全使用期間)が設定されており、鍵の更新周期は、当該鍵の安全使用期間から、当該鍵をもとに生成した電子署名の有効期間を減じた期間以下になるようにする。これは、鍵の解読がなされないうちに更新することで、鍵の安全性を確保しようとしたからである。なお、安全使用期間の設定は、鍵のセキュリティパラメータ、例えば鍵の長さ等を調整することによって行うことができる。電子署名の有効期間は、最初の分割区間と最後の分割区間のうち短い方の区間以下の長さの期間である。

【0034】図3は、各鍵の更新スケジュールを具体的に示した図である。主鍵と補助鍵との関係は、署名鍵SkT/確認鍵PkTで共通なので、一方の鍵についてのみ図示してある。ここでは、便宜上、2個の鍵の更新対象区間を共に1年、上記安全使用期間を5年、更新周期をすべて4年間隔とし、最初の1年及び最後の1年では補助鍵、中間の2年では主鍵として使用する。図中、「a0」、「a1」、「a3」、「a4」は、それぞれ鍵内容(値)である。

【0035】図3の例の場合、各鍵について、一方の鍵の使用区間が、他の鍵についての使用区間と時間的に連続し、且つ互いに重複しないようになっている。また、補助鍵である期間の和が使用区間と同一長さの期間であり、さらに、主鍵としての最初の1年と更新前の補助鍵としての最後の1年、及び、主鍵としての最後の1年と更新後の補助鍵についての最初の1年とが同一の期間となっている。これは、主として、鍵管理の容易性を考慮したためである。鍵更新は、一方の鍵が主鍵であり続ける最後の1年の始点で行う。そして、一方の鍵についての使用区間の終了時点で、更新された鍵についての使用区間を開始させるようにする。個々の更新対象区間における主鍵及び補助鍵の内容の組み合わせは、他の区間における組み合わせと異なっている。つまり、ある更新対象区間では、a0とa1、他の更新対象区間では、a1とa0、あるいはa1とa2、・・・、となっている。

【0036】上述の鍵更新が署名用の鍵(SkT)についてなされた場合、それと同期して、対応する確認用の鍵(PkT)も更新される。電子署名の生成、すなわち会員登録証の発行には、署名用主鍵を用い、電子署名の



確認、すなわち会員登録証の確認には確認用主鍵及び確認用補助鍵のペアのいずれかで行う。なお、各鍵の各々は、上記切り替えにかかわらず、署名用の鍵としての使用が可能なものである。

【0037】上記スケジュールで鍵更新がなされ、署名用主鍵を用いて発行された会員登録証の有効期間は、最長で1年、つまり1区間分となる。従って、前述のように、2人の会員U1、U2が相互の会員登録証L1、L2を確認しようとした場合、それらは、同じ区間で発行されたものか、1個だけ前後した区間で発行されたものである。2個離れた区間で発行された会員登録証は、どちらかが有効期間が切れたものとなる。また、有効期間の重なる2個の会員登録証を所持する会員は、確認用主鍵と確認用補助鍵のどちらかを使うことで、他の会員が所持する会員登録証を確認することができる。

【0038】また、確認用主鍵及び確認用補助鍵に当該鍵の使用終了期限を付加し、会員が他の会員の会員登録証を確認するときに、この使用終了期限が過ぎた鍵については、確認に使用しないようにすることも可能である。このようにすれば、使用終了期限の過ぎた鍵が解読されることによって行われる不正改竄にも、容易に対応できるようになる。

【0039】なお、図3の例では、2個の鍵の更新周期がすべて4年間隔であったが、図4及び図5に示すように、2個の鍵A、Bの更新周期がそれぞれ同一でない場合でも、本発明の鍵管理方法を実施することが可能である。

【0040】例えば、図4の鍵更新スケジュール例では、鍵A、Bの更新周期が5年、6年、5年、6年、・・・のように、周期的ではあるが、その周期が変化する。この例の場合、一方の鍵が主鍵として使用される区間で他方の鍵が補助鍵となる点は図3の例と同様であるが、各鍵についての使用区間が必ずしも一定ではない点が異なる。つまり、5年中2年の場合もあれば、5年中3年である場合もある。しかし、この場合も、一方の鍵を、他方の鍵が主鍵であり続けるうちに更新しておき、他方の鍵についての使用区間が終了した時点で更新後の鍵（それまでは補助鍵）についての使用区間を開始させるようにすることで、鍵更新をスムーズに行うことができるようになる。また、個々の鍵についての安全使用期間を上記更新周期よりも長くし、且つ電子署名の有効期間を、署名用主鍵として使用可能になった時点から1年以下とすることで、鍵の使用上のセキュリティも確保することができる。この場合の確認鍵も、確認用主鍵、確認用補助鍵のペアで公開し、確認者がペアの確認鍵のいずれかを用いて電子署名を確認できるようにする。

【0041】図5の鍵更新スケジュール例では、鍵Aの更新周期が5年、6年、5年、6年、・・・、鍵Bの更新周期が5年、5年、6年、6年、・・・のように周期が変化する。この場合も上記同様の規則に従って鍵更新

を行い、主鍵と補助鍵とを交互に切り替えることで、図3及び図4の例と同様の効果を期待することができる。

【0042】また、上述の例では、署名用及び確認用の鍵を2個づつ用意した場合の例であるが、本発明の鍵管理方法は、鍵が3個以上であっても実施することが可能である。例えば、5つの鍵を用いた場合の鍵更新スケジュール例を図6に示す。図6の例では、便宜上、5つの鍵A～Eがすべて5年周期で更新され、それぞれ1年毎に主鍵に切り替わるようにしている。つまり、補助鍵として使用する期間は、それぞれ使用区間（1年）の前後2年となる。各鍵A～Eの安全使用期間を7年以上とすれば、電子署名の有効期間は最大で2年とすることができ、図3の例（鍵が2個の場合）の有効期間（1年以下）よりも長くすることができる。

【0043】図6の鍵更新スケジュール例の場合、電子署名を生成した後、確認用に同時期に公開する確認鍵は、最大で5つとなる。この5つの確認鍵のいずれかを用いて電子署名を確認することができる点は、図3の例の場合と同様である。なお、各鍵A～Eの更新周期を、必ずしも同一長さとしなくとも良いことは、前述のとおりである。

【0044】次に、上記鍵管理方法を実施するための鍵管理システムについて説明する。この鍵管理システムは、会員システムの個々の機関、例えば前述の会員登録機関Tに、単独あるいは分散して備えられるもので、図7に示すように、演算処理装置1、表示出力装置2、データ入出力装置3、通信網接続装置4、情報処理制御部5、データファイル装置6、時間管理装置7、及び鍵生成装置8を有している。

【0045】演算処理装置1は、図示しない外部記憶装置やROMに記録されたプログラムを実行することで所要の機能を実現する一種のコンピュータであり、表示出力装置2は、演算処理装置1等による処理結果を視覚化するディスプレイ装置である。データ入出力装置3は、マウスその他のポインティングデバイスやキーボード等、外部記憶装置、及びこれらとの間のインタフェースを含むものである。通信接続装置4は、種々の会員やセンタCAとの間で行う通信を制御するものである。時間管理装置7はタイマ、鍵生成装置8は、鍵を生成する装置である。

【0046】情報処理制御部5は、例えば演算処理装置1が上記プログラムを読み込んで実行することにより形成される機能ブロックであり、図8(a)に示すように、モード更新の契機を付与する契機付与処理部51と、モード更新を行う更新処理部52と、主鍵・補助鍵の入れ替えを行う入れ替え処理部53と、主鍵・補助鍵の鍵内容を置換する置換処理部54と、電子署名を行う生成部55と、電子署名や主鍵・補助鍵を外部へ送信する送信処理部56とを有している。

【0047】契機付与処理部51では、一つの分割区間

の鍵内容を後続の分割区間に引き継ぐモードAと、直前の分割区間から後続の分割区間に移行する際に鍵内容を互いに置換するモードBとを選択的に適用するための契機を出力する。図3の鍵更新スケジュールに示した例では、1年が経過して2年目に移行する際にモードBが適用され、鍵内容a0、a1が主鍵・補助鍵で相互に置換される。2年目が経過して3年目に移行する際にモードAが適用され、主鍵の鍵内容a1は引き継がれるが、補助鍵の鍵内容a0は、「a2」に更新される。モードAとモードBは周期的に適用されるため、以下の説明では、モードA後、モードBが適用されるまでのサイクルをサイクルA、モードB後、モードAが適用されるまでのサイクルをサイクルBと称する場合がある。

【0048】更新処理部52は、上述のモード切換を行い、現在のサイクルを表すモードフラグ（サイクルA/B）をデータファイル装置6に記録しておき、以後のモード更新時（サイクル切替時）に参照できるようにしておく。入れ替え処理部53は、署名鍵及び確認鍵の各々について、主鍵と補助鍵とを入れ替えるものであり、置換処理部54は、鍵内容を新しいものに置換するものである。生成部55は、署名用主鍵を用いて、署名生成要求毎に指定された署名対象データの電子署名を行うものである。

【0049】データファイル装置6は、図8(b)に示すように、モードフラグ61、確認用主鍵62、署名用主鍵63、確認用補助鍵64、署名用補助鍵65がそれぞれ格納されている。会員登録機関Tが確認用主鍵62と確認用補助鍵64を保持するのは、センタCAによらず、直接会員に確認鍵を配布する場合があるためである。

【0050】次に、上記鍵管理システムを応用した会員システムの運用形態を説明する。この会員システムは、図9の概略図に示すように、それぞれ会員であるチケット販売機関B、利用者会員U、サービス提供者Iを、通信網を通じて会員登録機関Tに接続して構成される。本発明の鍵管理システムは会員登録機関Tに設けられるが、他の会員も同時に備えるように構成してもよい。各会員は、少なくとも暗号技術を用いた認証通信が可能であるものとする。この会員システムの運用手順は、図10～図12に示すとおりである。

#### 【0051】(1) 会員登録

図10を参照し、会員登録機関Tは、まず鍵の更新を行う日を設定する（例えば、毎年1月1日）。また、確認用主鍵PkTm62、署名用主鍵SkTm63と、確認用補助鍵PkTs64、署名用補助鍵SkTs65を用意し、モードフラグ61を「サイクルA」に設定する（ステップS201）。利用者会員Uは、自らの署名鍵SkUと確認鍵PkUとを作り、確認鍵PkUと利用者名などの会員情報IdUとからなる会員登録請求情報を会員登録機関Tへ送信する（ステップS202）。

【0052】会員登録機関Tでは、この送信された会員登録請求情報から確認鍵PkUを抽出して、鍵管理システムの生成部55により、これに有効期限Euをつけたものを署名対象データとする。そして、署名用主鍵SkTmを用いてこの署名対象データに署名して会員登録証Luを発行する。その後、送信処理部56により、会員登録証Luを、有効期限Eu、確認鍵PkU、会員情報IdU、及び前述の確認用主鍵PkTm62、確認用補助鍵PkTs64と共に、利用者会員Uへ送信する（ステップS203）。

【0053】会員登録機関Tは、会員登録の請求をいつでも受付可能にすることができて、会員登録の日から1年間有効な会員登録証Luを発行する。チケット販売機関B、サービス提供者Iも、同様にして、会員登録を行い、会員登録証Lb、Liの発行を受ける。

【0054】1回目の鍵更新の日（1月1日）が到来すると、会員登録機関Tは、モードフラグ61を参照し、更新処理部52で現在のサイクルAをサイクルBに更新する（ステップS204）。続いて、入れ替え処理部53で、主鍵と補助鍵とを入れ替える（ステップS205）。

【0055】2回目の鍵更新の日（翌年の1月1日）が到来すると、会員登録機関Tは、更新処理部52で現在のサイクルBをサイクルAに更新する（ステップS206）。続いて、鍵生成装置8で生成した新しい鍵を、置換処理部54で補助鍵として保存する（ステップS207）。これを更新周期である4年間の間に、もう1サイクルずつ繰り返す（ステップS208～S211）。

【0056】利用者会員U、チケット販売機関B、サービス提供者Iへの確認用の鍵の配布（確認用主鍵PkTm62、確認用補助鍵PkTs64の送信）は、安全のためにオフラインでの処理を含めることが望ましい。例えば、対面で手渡しするとか、郵送や、ファクシミリなどで送るなどの方法を併用すると、より安全になる。オンラインでのみ行う場合は、何等かの認証通信を行う必要がある。センタCAの公開鍵証明書を利用する場合、通常の公開鍵証明書には、公開鍵である確認鍵は1個しか含まれないため、公開鍵証明のフォーマットを修正して公開鍵を2個含めるようにする方法と、公開鍵証明書を2個利用する方法がある。これによって、センタCAの公開鍵証明書を利用することができる。

#### 【0057】(2) サービス提供情報の登録

図11を参照し、サービス提供者Iは、サービス提供保証情報C、チケット販売機関Bの確認鍵PkB、サービスの有効期限Ec、チケットの発行通番Rc、会員情報IdI、その他サービス内容・金額など、必要に応じた項目情報をチケット販売機関Bへ送信する（ステップS301）。これは、サービス提供者Iが、事後的に送られたチケットの真偽を事後的に確認できるようにする情報である。このような情報を予めチケット販売機関Bに

登録しておくことで、利用者会員Uによるチケットの2重使用や、チケット販売機関Bが不正した場合に、サービス提供前に、検出可能になるというメリットがある。

【0058】(3) チケットの販売

利用者会員Uとチケット販売機関Bとの間で、相互に会員登録証L<sub>u</sub>、L<sub>b</sub>を確認する場合は、次のような手順となる。利用者会員Uは、まず、会員登録証L<sub>u</sub>、確認鍵P<sub>kU</sub>、有効期限E<sub>IU</sub>、及びチャレンジ(認証依頼)を、チケット販売機関Bへ送信する(ステップS302)。ここではチャレンジは、暗号化技術・署名技術の一例として使用されている。

【0059】チケット販売機関Bは、利用者会員Uから送られてきた会員登録証L<sub>u</sub>等を、自分の保管している確認用主鍵P<sub>kTm</sub>・確認用補助鍵P<sub>kTs</sub>の両方で試す(ステップS303)。利用者会員Uの会員登録証L<sub>u</sub>と、チケット販売機関Bの会員登録証L<sub>b</sub>は、どちらが先に発行されたものであっても、また、先の発行と後の発行との間に、会員登録機関Tが、署名鍵を更新した場合であってもよい。両方とも有効な会員登録証L<sub>u</sub>、L<sub>b</sub>である限り、どちらか片方の確認鍵で、署名の確認ができる。公開鍵証明書発行センタCAに公開鍵証明書を取りにいたり、利用者から送信する必要はない。どちらか片方の確認鍵で、署名の確認ができれば、次の処理に進む。確認できなかった場合は、会員登録証L<sub>u</sub>が有効ではないことを意味するので、チケットの販売を拒否する(ステップS304: No、S305)。

【0060】次に、チケット販売機関Bは、自分の会員登録証L<sub>b</sub>、確認鍵P<sub>kB</sub>、有効期限E<sub>IB</sub>、及び利用者会員Uから送られてきたチャレンジに対して、チケット販売機関Bの署名鍵S<sub>kB</sub>を用いて生成した署名を利用者会員Uへ送信する(ステップS306)。利用者会員Uは、チケット販売機関Bから送られてきた会員登録証L<sub>b</sub>を、自分の保管している確認用主鍵P<sub>kTm</sub>・確認用補助鍵P<sub>kTs</sub>の両方で試す(ステップS307)。どちらか片方の確認鍵で、署名の確認ができれば、次の処理に進む。確認できなかった場合は、会員登録証L<sub>b</sub>が有効ではないことを意味し、偽りのチケット販売機関である可能性があるので、購入を取り止める(ステップS307: No、S308)。

【0061】会員登録証L<sub>b</sub>の確認ができれば、自分の送ったチャレンジに対するチケット販売機関Bの署名をチケット販売機関Bの確認鍵P<sub>kB</sub>で確認する。確認できた場合は、次に進む。なお、確認鍵P<sub>kB</sub>がチケット販売機関Bの正当な公開鍵であることは、チケット販売機関Bの会員登録証L<sub>b</sub>を確認することで確認されている。利用者会員Uは、購入したいチケットの情報Hにチケットの情報とチケット販売機関Bが生成したチャレンジに対する利用者会員Uの署名鍵にて生成した電子署名を添付して、チケット販売機関Bへ送信し、チケットの購入を申し込む(ステップS309)。

【0062】チケット販売機関Bは、利用者会員Uから送られてきたチケット情報とその電子署名を、利用者会員Uの確認鍵P<sub>kU</sub>にて確認する(ステップS310)。チケット情報とその電子署名の確認ができた場合は、次の処理に進む(ステップS311: Yes)。確認できなかった場合は、会員登録証L<sub>u</sub>の正当な所持者以外のものが購入の申込みをしているか、通信中にデータが改竄されていることを意味するので、チケットの販売を拒否する(ステップS311: No、S312)。

【0063】チケット販売機関Bは、また、利用者会員Uの確認鍵P<sub>kU</sub>、サービス提供保証情報C、有効期限E<sub>c</sub>、発行通番R<sub>c</sub>、会員情報I<sub>dI</sub>、チケット販売機関Bのチケット販売通番R<sub>f</sub>、及びチケット有効期限E<sub>f</sub>を合わせたものを署名対象データとして、チケット署名情報Fを生成する。ここでチケット署名情報Fは、チケット毎に別々の値にならないため、署名対象データにチケット販売通番R<sub>f</sub>を含めるようにする。その後、サービス提供者Iの会員登録証L<sub>i</sub>、確認鍵P<sub>kI</sub>、及び有効期限E<sub>II</sub>と、チケット販売通番R<sub>f</sub>、チケット有効期限E<sub>f</sub>、及びチケット署名情報Fを利用者会員Uへ送信する(ステップS313)。

【0064】利用者会員Uは、サービス提供者Iの会員登録証L<sub>i</sub>を会員登録機関Tの確認鍵P<sub>kT</sub>でチェックする。会員登録証L<sub>i</sub>の確認ができた場合は、サービス提供者Iの確認鍵P<sub>kI</sub>で上記サービス提供保証情報Cを確認し、さらに、チケット販売機関Bの確認鍵P<sub>kB</sub>で上記チケット署名情報Fを確認する。チケット署名情報F等の確認ができた場合は、料金\$の支払いを行う(ステップS314)。

【0065】(4) チケットの使用

図12を参照し、利用者会員Uは、会員登録証L<sub>u</sub>、確認鍵P<sub>kU</sub>、有効期限E<sub>Iu</sub>とチャレンジを、サービス提供者Iへ送信する(ステップS401)。サービス提供者Iは、チケット販売機関Bと同様に利用者会員Uの会員登録証L<sub>u</sub>を確認する(ステップS402)。確認できた場合は、サービス提供者Iの会員登録証L<sub>i</sub>、チャレンジに対する電子署名、及びチャレンジを利用者会員Uへ送信する(ステップS403: Yes、S405)。

【0066】利用者会員Uもサービス提供者Iの会員登録証L<sub>i</sub>を確認し、チャレンジの電子署名を確認する(ステップS406)。確認できた場合(ステップS407: Yes)、利用者会員Uは、チケット署名情報Fとサービス提供者Iの確認鍵とチャレンジを合わせたものに、自分の署名鍵で、利用者署名情報S、会員登録証L<sub>b</sub>、確認鍵P<sub>kB</sub>、有効期限E<sub>IB</sub>、チケット署名情報F、チケット販売通番R<sub>f</sub>、有効期限E<sub>f</sub>、サービス提供保証情報C、発行通番R<sub>c</sub>、有効期限E<sub>c</sub>、会員情報I<sub>dI</sub>の電子署名を生成して、サービス提供者Iへ送信する(ステップS407: Yes、S409)。

【0067】サービス提供者Iは、サービス提供保証情報C、チケット署名情報F、利用者署名情報S、チケット有効期限E f、E c、及びチケットが既にしようされていないかどうかを確認する。確認できた場合は、サービス提供を開始する（ステップS 410）。サービス提供者I、利用者会員Uの相互認証の結果が否定的であった場合は、サービス提供や申し込みが拒否される（ステップS 403: No, S 404、S 407: No, S 408）。

【0068】（5）チケットの譲渡

また、会員間で、次のようにやり取りすることで、チケットの譲渡をすることも可能である。会員U1は、チケットに譲渡証明を示す署名をつけて、会員U2に渡す。会員U2は、チケットと譲渡証明を、サービス提供者Iへ送信する。サービス提供者Iは、チケットと譲渡証明とを確認して、会員U2にサービスを提供する。

【0069】なお、会員システムを運用する場合において、利用者会員Uが提示した会員登録証が、会員登録機関Tから発行されたものかどうか、あるいは電子署名が正当かどうかを、上記チケット販売機関Bやチケット提供者Iとは別に、確認する必要がある場合がある。この場合は、本発明の認証システムを用いて当該会員登録証の正当性を確認する。この認証システムは、電子署名と複数の確認鍵とを受領してその内容を確認する第1の確認処理部と、受領した電子署名を複数の確認鍵のいずれかで確認する第2の確認処理部とを備え、第2の確認処理部で確認がとれた場合は、その電子署名が正当なものと判定する。これらの確認処理部は、例えばコンピュータが所定のプログラムを読み込んで実行することによって当該コンピュータ内に形成される機能ブロックである。なお、受領した電子署名は、異なる時期に更新された署名鍵によって生成されたものであっても良い。

【0070】次に、図13を参照して、会員システムの他の構成例を示す。基本的な動作は図9に示した構成の会員システムと同様であるが、ここでは、本発明の鍵管理システムを、会員登録機関Tのほか、チケット販売機関Bにも設けている。また、図9に示した構成の会員システムでは、チケット販売機関Bの鍵は1組であるが、ここでは、2組の鍵でもって会員登録証Lの発行を請求するようにする。

【0071】すなわち、チケット販売機関Bでは、チケット用の署名鍵（SkBm/SkBs：以下、チケット署名鍵）を主鍵と補助鍵の2個用意し、これを、例えば図3に示したような鍵管理スケジュールで更新するようにする。なお、会員登録証Lの更新契機とチケット署名鍵の更新契機は、同一である必要はないが、同一でも構わない。但し、チケット署名鍵は、会員登録証Lの有効期間と同じかそれ以上の有効期間をもつことが必要である。ここでは、会員登録証Lの更新契機で、当該会員登録証Lと同じ長さの有効期間を持つチケット署名鍵を使

用する。例えば、4月1日に会員登録することにして、1年毎に更新を行うこととする。

【0072】チケット販売機関Bの会員登録証L bの有効期限E l bが切れたとき、そのときのチケット販売機関Bの確認鍵PkBm/PkBsを会員登録機関Tに送り、新たな会員登録証L bを発行してもらう。サービス提供者Iは、サービス提供保証情報Cをチケット販売機関Bに預けるのを契機にして、チケット販売機関Bの会員登録証L bと、確認鍵PkBm/PkBsと、有効期限E l bとを入手する。サービス提供保証情報Cの有効期限E cは、例えば発行後1年以下とする。会員登録証L bの署名を確認できたら、会員登録証L b、確認鍵PkBm/PkBs、及び有効期限E l bを保管する。

【0073】利用者会員Uは、チケットの購入を契機にして、チケット販売機関Bの会員登録証L bを入手する。ここで入手したチケット販売機関Bの会員登録証L bは、チケットの確認後は、保管する必要がなくなることが、チケット販売機関Bに、本発明の鍵管理システムを用いた場合のメリットの一つである。

【0074】利用者会員Uは、チケットを、サービス提供者Iへ送信する。ここでは、サービス提供保証情報C、チケット署名情報F、利用者署名情報S、会員登録証L u、有効期限E c、発行通番R c、会員情報I d、チケット販売通番R f、有効期限E f、確認鍵PkU、有効期限E l uを送信することになる。サービス提供者Iは、チケット販売機関Bの会員登録証L bを入手した後、利用者会員Uが、チケット販売機関Bの署名を入手するまでの間に、サービス提供者Iの鍵の更新が行われた場合でも、チケット販売機関Bの主鍵か補助鍵のどちらかで、会員登録証L bを確認することができるので、再度鍵を取得する処理を行う必要はない。

【0075】次に、鍵更新スケジュールについて説明する。この場合も会員登録機関Tは、1年毎に鍵を更新するものとする。但し、上述したように、会員登録機関Tは、5年間有効の1個の鍵を2年毎に生成するものであり、この1個の鍵は、最初と最後の区間、すなわち1年目と4年目の区間で補助鍵として使用し、その間の2区間、すなわち2年目と3年目の区間で主鍵として使用する。このとき、会員登録証の有効期間は1年間、若しくは1年未満とする。チケット販売機関Bは、会員登録機関Tとは異なるタイミングで鍵の更新を行う。このときの周期は同じ1年毎とする。また、チケット署名情報Fの有効期間は1年間、若しくは1年未満とする。

【0076】会員登録機関Tとチケット販売機関Bは、それぞれ鍵を更新すると、これをセンタCAに登録する。これは、認証通信の代用とするためである。このようにセンタCAへ登録する場合、利用者会員U及びサービス提供者Iは、会員登録証Lの更新や、サービス提供保証情報Cの登録や、チケット署名情報Fの購入を契機に、会員登録機関Tやチケット販売機関Bの鍵をセンタ

CAから取得できるようになる。

【0077】以下、実際の鍵更新の様子を図14のスケジュール例に従って説明する。ここでは、サービス提供保証情報Cの預入時にサービス提供者Iとチケット販売機関Bとの間で、チケットの購入時に利用者会員Uとチケット販売機関Bとの間で、チケット使用時に利用者会員Uとサービス提供者Iとの間で、それぞれ会員登録機関Tが発行した会員登録証が確認でき、かつチケットの使用時に、チケット販売機関Bが発行したチケット署名情報Fが確認できることを要点とする。

【0078】図14では、最初の区間(1年目)での確認鍵PKT1の内容は、主鍵がt0、補助鍵がt1であるとする。2番目の区間での確認鍵PKT2は、主鍵と補助鍵とが入れ替えられ、主鍵はt1、補助鍵はt0となる。さらに、3番目の区間での確認鍵PKT3は、主鍵はt1のまま、補助鍵は新しく生成された内容t2となる。

【0079】利用者会員Uの会員登録証L1は、3番目の区間で発行される。具体的には、当該区間での確認鍵PKT3の主鍵t1に対応する署名鍵SKT3の主鍵で生成される。このとき、当該区間での確認鍵PKT3の主鍵t1と補助鍵t2とが利用者会員Uに配布される。また、会員登録証L2は、4番目の区間で発行される。具体的には、当該区間での確認鍵PKT4の主鍵t2に対応する署名鍵SKT4の主鍵で生成される。このとき、確認鍵PKT3の主鍵t2、補助鍵t1が利用者会員Uに配布される。サービス提供者Iの会員登録証L1、L2、L3、...、チケット販売機関Bの会員登録証L1、L2、L3、...、についても同様である。但し、ここではチケット販売機関Bの鍵も本発明の鍵管理方法で鍵更新を行っている。図14でチケット販売機関Bの横に記載されているPKB1、PKB2、...、の部分は、このことを意味している。チケット販売機関Bは、主鍵と補助鍵を合わせた確認鍵を、会員登録機関Tに送り、会員登録証を発行してもらう。

【0080】次に、利用者会員Uとサービス提供者Iとの間の認証について説明する。利用者会員Uの会員登録証L2は、t1の署名鍵で発行されている。それと重なる有効期間を持つサービス提供者Iの会員登録証L2は、発行時に、主鍵t1、補助鍵t2を取得しているため、利用者会員Uの会員登録証L1を主鍵t1で確認することができる。また、サービス提供者Iの会員登録証L2は、主鍵t2、補助鍵t1を取得しているため、今度は利用者会員Uの会員登録証L1の署名内容を補助t1で確認することができる。

【0081】逆に、利用者会員Uは、会員登録証L1の発行時に主鍵t1、補助鍵t2を取得しているため、主鍵t1で生成されているサービス提供者Iの会員登録証L1や、主鍵t2で生成されている会員登録証L2を確認することができる。利用者会員Uは、また、会員登録

証L2の時は、主鍵t2、補助鍵t1を取得しているため、主鍵t2にてサービス提供者Iの会員登録証L2を確認することができる。サービス提供者Iとチケット販売機関B、利用者会員Uとチケット販売機関Bについても同様に確認を行うことができる。

【0082】このように、会員登録証の発行はいつでも行うことができ、また、サービス提供者Iとチケット販売機関B、利用者会員Uとチケット販売機関B、利用者会員Uとサービス提供者Iとの間で、お互いの会員登録証Lが有効である限り、いつでも、どの組み合わせでも相手の会員登録証Lを、自分の持っている鍵(PKTn)で確認することができる。

【0083】次に、チケット署名情報Fについて、より詳細に説明する。チケット販売機関Bでは、確認鍵PKB1、確認鍵PKB2、...の順に鍵更新しているものとする。すなわち、前述の会員登録機関Tが確認鍵PKT1、確認鍵PKT2、...と更新するのと同様の規則に従って鍵更新を行う。サービス提供者Iは、サービス提供保証情報Cをチケット販売機関Bに登録する。これを契機にして、チケット販売機関Bの主鍵・補助鍵を入手する。サービス提供保証情報C、チケット署名情報Fの有効期間は、例えば1年とする。利用者会員Uが、チケットを購入する場合、チケット販売機関Bは、確認鍵PKB3の主鍵b1の署名鍵で、チケット署名情報F1を生成する。一方、サービス提供者Iは、サービス提供保証情報Cをチケット販売機関Bに登録する際に、チケット販売機関Bの確認鍵PKB2か、確認鍵PKB3のどちらかを入手している(なぜならば、サービス提供保証情報Cの有効期間が1年)。また、利用者会員Uがチケット署名情報F1を使用する前に、確認鍵PKB4を入手している場合もある。いずれにしても、サービス提供者Iは、利用者会員Uがチケット署名情報F1を使用する時点で、確認鍵PKB2、確認鍵PKB3、確認鍵PKB4のいずれかを持っていて、その主鍵か補助鍵のどちらかにb1が入っているため、署名確認ができる。

【0084】また、利用者会員Uが、チケットを購入する場合の2つ目の例を挙げる。この場合、チケット販売機関Bは、確認鍵PKB4の主鍵b2の署名鍵で、チケット署名情報F2を生成する。一方、サービス提供者Iは、サービス提供保証情報Cをチケット販売機関Bに登録する際に、チケット販売機関Bの確認鍵PKB3か、確認鍵PKB4のどちらかを入手している。また、利用者会員Uがチケット署名情報F1を使用する前に確認鍵PKB5を入手している場合もある。いずれの場合にも、サービス提供者Iは、利用者会員Uがチケット署名情報F1を使用する時点で、確認鍵PKB3、確認鍵PKB4、確認鍵PKB5のいずれかを持っていて、その主鍵か補助鍵のどちらかにb2が入っているため、署名の確認ができる。

【0085】このように、チケット販売機関Bの署名鍵を更新することで、チケット販売機関Bが利用者会員Uに対して発行する署名Fをサービス提供者Iは、いつでも確認することができる。

【0086】

【発明の効果】以上の説明から明らかなように、本発明によれば、署名鍵に用いる鍵を複数個用意し、これらの鍵を一定規則で更新するとともに、確認鍵もこれらの鍵の更新に同期させて更新して公開するようにしたので、更新の際に電子署名の発行を停止させたり、鍵の更新後のサービスの利用を制限する必要がなくなる。また、認証時にオンラインで鍵を取り寄せたり、公開鍵証明書を取得する必要もなくなる。さらに、異なる時期に発行された電子署名の相互認証をオフラインで行うことも可能になった。

【図面の簡単な説明】

【図1】本発明が適用される会員システムの概略構成図。

【図2】図1の構成による鍵等の配送シーケンスを示す手順説明図。

【図3】鍵更新スケジュールの最も単純な例を示したシーケンスチャート。

【図4】周期が変化する場合の鍵更新スケジュールの例を示したシーケンスチャート。

【図5】周期が変化する場合の他の鍵更新スケジュールの例を示したシーケンスチャート。

【図6】5個の鍵を用いる場合の鍵更新スケジュール例

を示したシーケンスチャート。

【図7】本発明の鍵管理システムの構成例を示すブロック図。

【図8】(a)は鍵管理システムにおける情報処理制御部の詳細ブロック図、(b)はデータファイル装置の詳細構造図。

【図9】本実施形態の会員システムの運用形態を示すブロック図。

【図10】図9の形態の会員システムにおける鍵配送及び鍵更新の手順説明図。

【図11】図9の形態の会員システムにおける会員間の相互認証の手順説明図。

【図12】図9の形態の会員システムにおける会員間の相互認証の手順説明図。

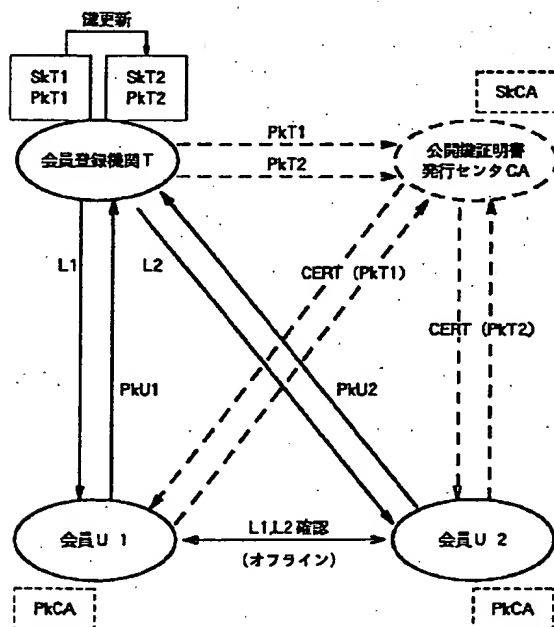
【図13】本実施形態の他の会員システムの運用形態を示すブロック図。

【図14】図13の形態の会員システムにおける鍵更新のスケジュール例を示したシーケンスチャート。

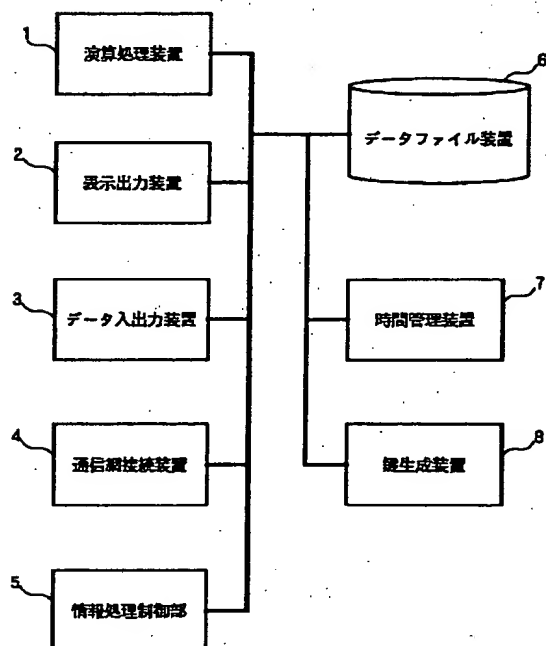
【符号の説明】

- 1 演算処理装置
- 2 表示出力装置
- 3 データ入出力装置
- 4 通信網接続装置
- 5 情報処理制御部
- 6 データファイル装置
- 7 時間管理装置
- 8 鍵生成装置

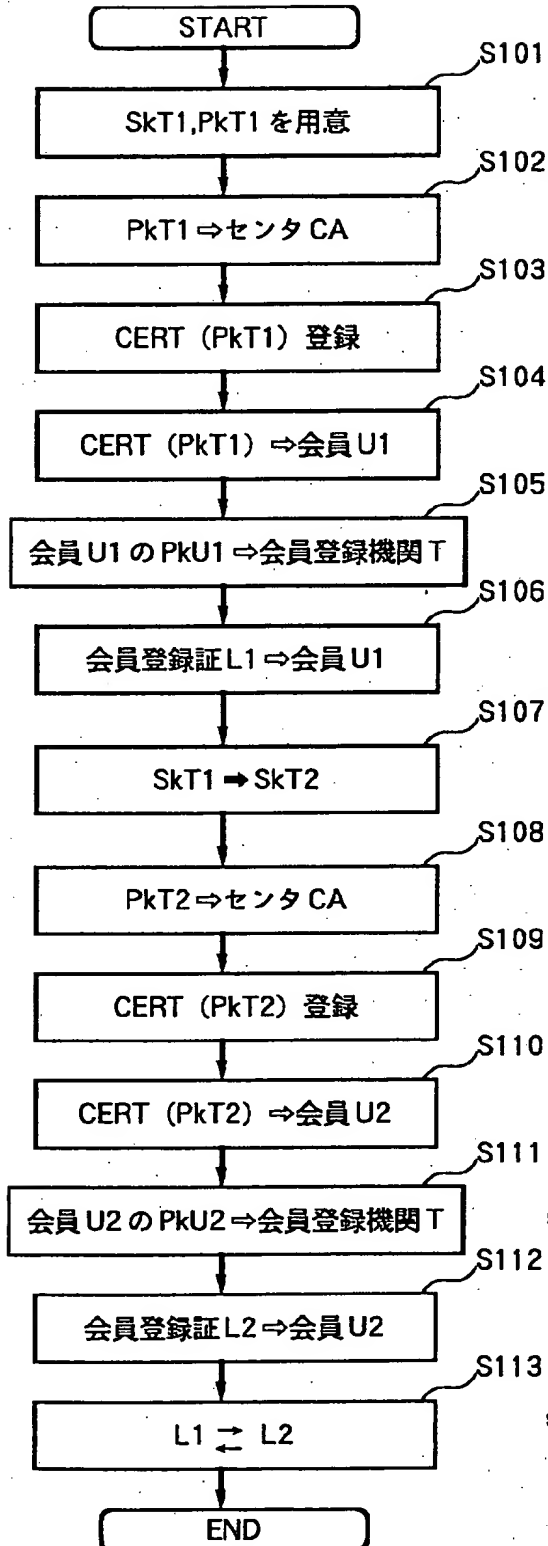
【図1】



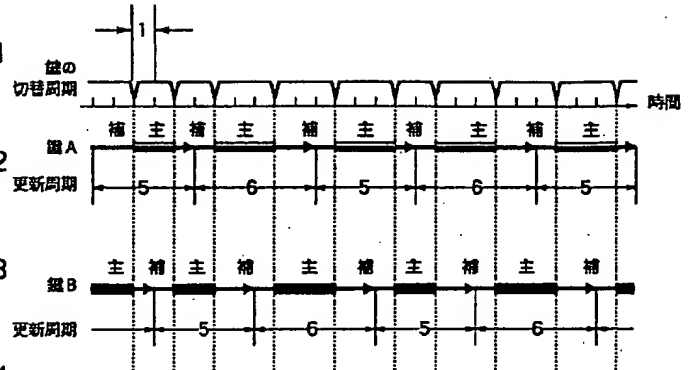
【図7】



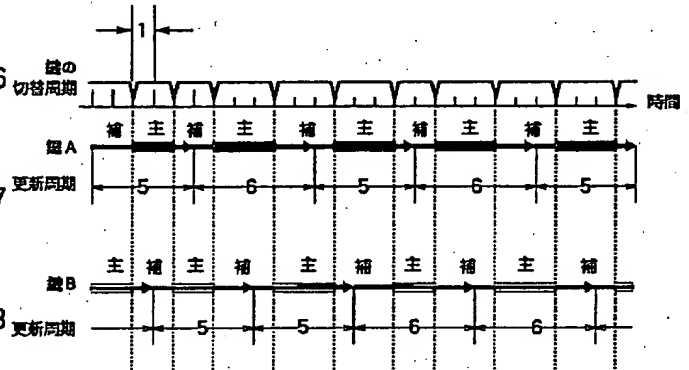
【図2】



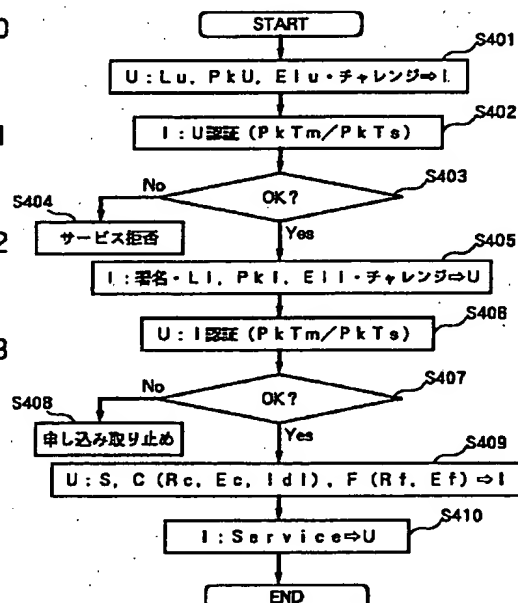
【図4】



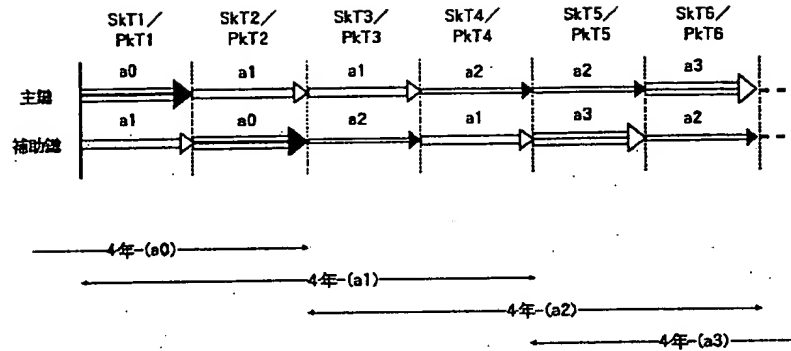
【図5】



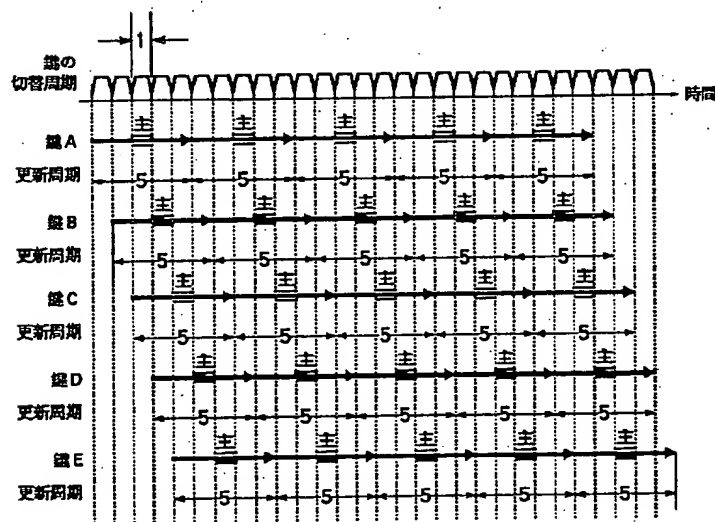
【図12】



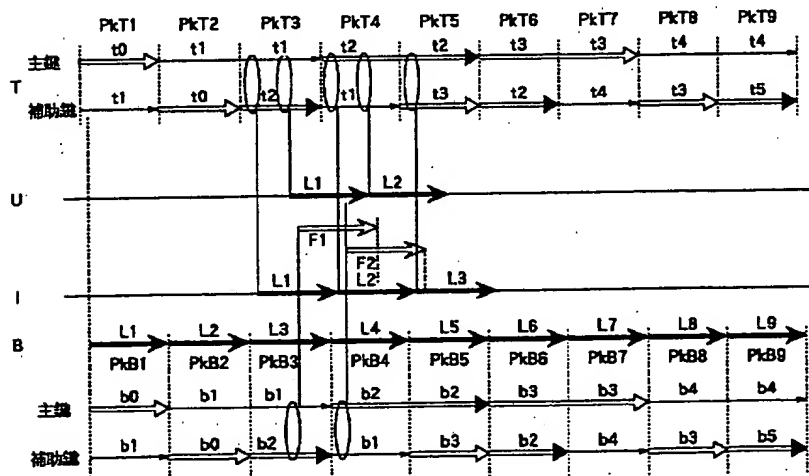
【図 3】



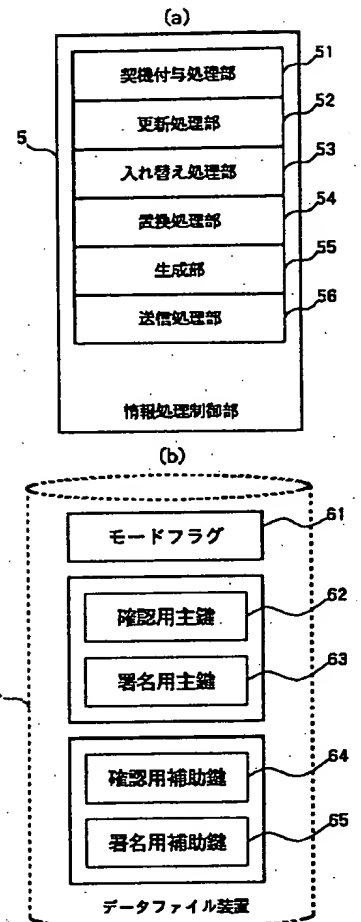
【図 6】



【図 14】



【図 8】





[illegible]

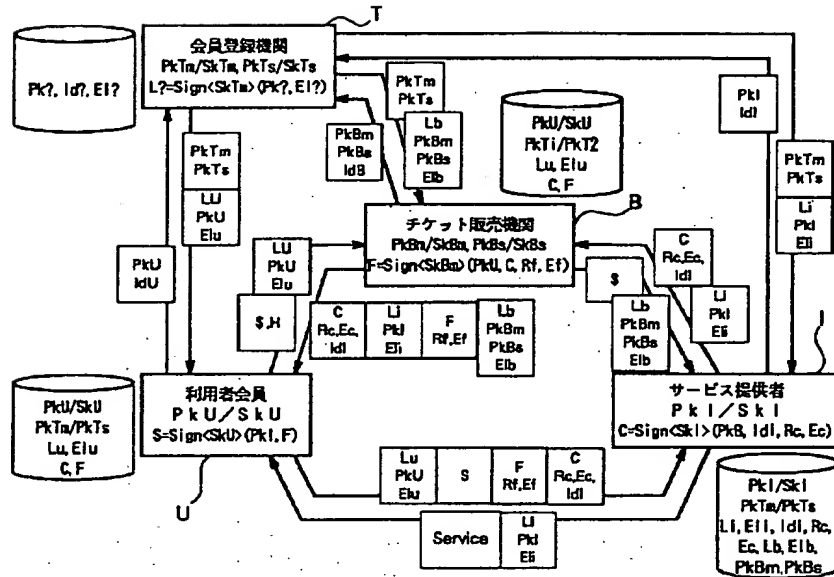
The flowchart illustrates a 4-year cycle process. It begins with a box labeled 'START'. A vertical line on the left indicates the progression of years: '1年目' (Year 1), '2年目' (Year 2), '3年目' (Year 3), and '4年目' (Year 4). The process steps are as follows:

- Year 1:**
  - S201:  $T: SkTm, SkTs, PkTm, PkTs$  を用意: サイクルA
  - S202:
    - $U: PkU, IdU \Rightarrow T$
    - $B: PkB, IdB \Rightarrow T$
    - $I: PkI, IdI \Rightarrow T$
  - S203:
    - $T: Lu, Elu, PkTm, PkTs \Rightarrow U$
    - $T: Lb, Elb, PkTm, PkTs \Rightarrow B$
    - $T: Li, Eli, PkTm, PkTs \Rightarrow I$
  - S204: サイクルA  $\Rightarrow$  B
- Year 2:**
  - S205: 主盤  $\rightleftharpoons$  補助盤
- Year 3:**
  - S206: サイクルB  $\Rightarrow$  A
  - S207: T: 新しい補助盤作成・保存
- Year 4:**
  - S208: サイクルA  $\Rightarrow$  B
  - S209: 主盤  $\rightleftharpoons$  補助盤
  - S210: サイクルB  $\Rightarrow$  A
  - S211: T: 新しい補助盤作成・保存
- The process concludes with an 'END' box.

```

graph TD
    START([START]) --> S301[S301 I: C (Ee, Rc, Idl), Pk B ⇒ B]
    S301 -.-> S302[S302 U: Lu, Pk U, El u・チャレンジ ⇒ B]
    S302 --> S303[S303 B: U 認証 (Pk Tm / Pk Ts)]
    S303 --> S304{S304 OK?}
    S304 -- No --> S305[S305 販売拒否]
    S304 -- Yes --> S306[S306 B: 署名・Lb, Pk B, El b・チャレンジ ⇒ U]
    S306 --> S307[S307 U: B 認証 (Pk Tm / Pk Ts)]
    S307 --> S308{S308 OK?}
    S308 -- No --> S309[S309 購入取り止め]
    S308 -- Yes --> S309[S309 U: 署名・チケット情報申し込み, H ⇒ B]
    S309 --> S310[S310 B: U 認証 (Pk U)]
    S310 --> S311{S311 OK?}
    S311 -- No --> S312[S312 販売拒否]
    S311 -- Yes --> S313[S313 B: C, Li, Rf, Ef, F ⇒ U]
    S313 --> S314[S314 U: S ⇒ B]
    S314 --> END([END])
  
```

【図13】



フロントページの続き

(51) Int. Cl. 6

識別記号

F I

H 0 4 L 9/00

6 0 1 F